Cisco Registered Envelope Service

Cisco® Registered Envelope Service は、非常に高度なクラウド ベースの暗号キー サービスです。柔軟性と拡張性の高いこのサービスは、コンプライアンス要件への準拠、通信の保護、または知的財産の保護のいずれが必要な場合でも、インフラストラクチャへの追加投資をせずにメッセージに関連した要件に対応できるようサポートします。

製品概要

Cisco E メールおよび Web セキュリティ製品は、あらゆる規模の企業を保護するために設計された、高性能で使いやすく、革新的な技術を取り入れたソリューションです。世界の最も重要なネットワークを保護することを目的として設計されたこの商品をゲートウェイに配置することにより、境界の強力な防御機能を実現できます。

アプライアンスの製品ラインは、Cisco Security Intelligence Operations および Global Threat Correlation を活用しているため、よりスマートかつ高速です。この高度なテクノロジーにより、組織はセキュリティを向上させ、ユーザを最新のインターネット脅威から保護することができます。

機能

通常の E メールは安全性の高い情報交換手段と言えませんが、大抵の場合、暗号化やキー管理は、日常の通信手段として使用するには複雑過ぎます。Registered Envelope Service は、暗号化の複雑さを取り払い、安全性の高いメッセージを簡単に送受信できるようにします。

安全な配信方法

このサービスは、メッセージ配信のための多様な選択肢を提供し、どんな E メール暗号化要件にも対応します。

シスコの E メール暗号化は、極めて安全なエンベロープ ベースの「プッシュ」テクノロジーであり、どこからでも利用でき、簡単に使用できるにもかかわらず、総所有コスト（TCO）は大きくありません。暗号化されたメッセージは、使用している E メール クライアント、オペレーティング システムまたはデバイスにかかわりなくすべての E メール ユーザが受信できます。また何らかのソフトウェアをインストールする必要も、送信者が暗号化のクレデンシャルを受信者と事前に交換する必要もありません。

ビジネスクラスの電子メール

暗号化テクノロジーは、E メール コンテンツを保護するだけでなく、E メールの可視性と制御を強化します。

保証された開封確認により、ユーザはメッセージがそれぞれの受信者によっていつ開封されたかを正確に知ることができます。

メッセージの期限切れと取り消しは、誤送信されたメッセージが開かれることを防ぎ、古いメッセージを自動的に保護します。メッセージはいつでも取り消しできます。

認証とキーの配信は通常、ユーザ クレデンシャルを識別することにより実施されます。受信者が認証されると、そのメッセージのキーがリリースされて、受信者がメッセージにアクセスできるようになります。

登録管理は初めてメッセージを受信するときに表示されるもので、単一のスクリーンから、キー サーバにアカウントを作成するように誘導されます。それ以降は、このアカウントを使用してメッセージを受信できます。

Security Assertion Markup Language（SAML）2.0 ゲートウェイ統合は、アイデンティティ ゲートウェイを実装した組織向けの拡張機能であり、この拡張機能を通して組織はサービスへの既存の投資を活用できます。暗号化エンベロープの受信者は、企業のクレデンシャルを使用してサービス認証をし、メッセージを自動的に復号化します。この統合が使用されている場合は、企業のユーザ名とパスワードを使用して保護されたメッセージに簡単にアクセスすることができ、メッセージを初めて受信するときにサービスで新しいアカウントを作成する必要がありません。

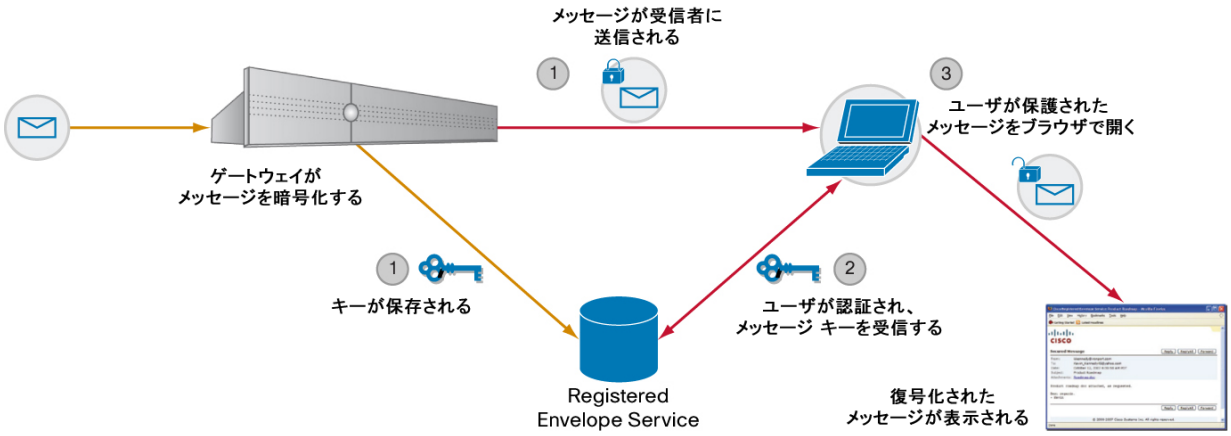
ユニバーサル デバイス サポートにより、メッセージの開封に使用するデバイスにかかわりなく、すべての受信者が安全性の高いメッセージを読むことができます。専用のプラグイン アプリケーションは、Microsoft Outlook に対して、また Apple iOS および Google Android スマートフォン上での優れたユーザ エクスペリエンスを提供します。

メッセージ管理は、メッセージの取り消しや有効期限、および開封通知を含みます。これらの機能には、サービスの Web インターフェイスから、または専用プラグインをインストールすることにより E メール クライアントから直接アクセスできます。

Hosted Key Server

Registered Envelope Service は、受信者の登録、認証、およびメッセージごとの暗号キーを管理します。図 1 は、E メール セキュリティ アプライアンスと Registered Envelope Service のやり取りを示しています。C シリーズ アプライアンスで定義されたポリシーに従ってメッセージを暗号化し、復号化します。

図 1. 暗号化されたビジネスクラスの E メールのパス



利点

コンプライアンス遵守をサポート

機密性の高いメッセージは、医療保険の相互運用性と説明責任に関する法令（HIPAA）、Sarbanes-Oxley 法（SOX）、Gramm-Leach-Bliley 法（GLBA）、個人情報保護および電子文書法（PIPEDA）、EU データ指令などの規制法令に準拠しつつ処理されます。

フェデレーテッド アイデンティティ ゲートウェイの使用

SAML 2.0 ゲートウェイとの互換性により、新規受信者登録の必要がなくなり、受信者は自社のアイデンティティを使用してメッセージを復号できます。

ビジネスクラスの E メールの提供

強力な機能により、優れた可視性と制御で新しいクラスの E メールがサポートされます。

お客様およびパートナーとの信頼関係の促進

暗号化は、お客様やパートナーへのサービスのレベルを向上し、ビジネス上の取引と通信の機密性を保つというシスコの約束を実証します。

知的所有権の保護

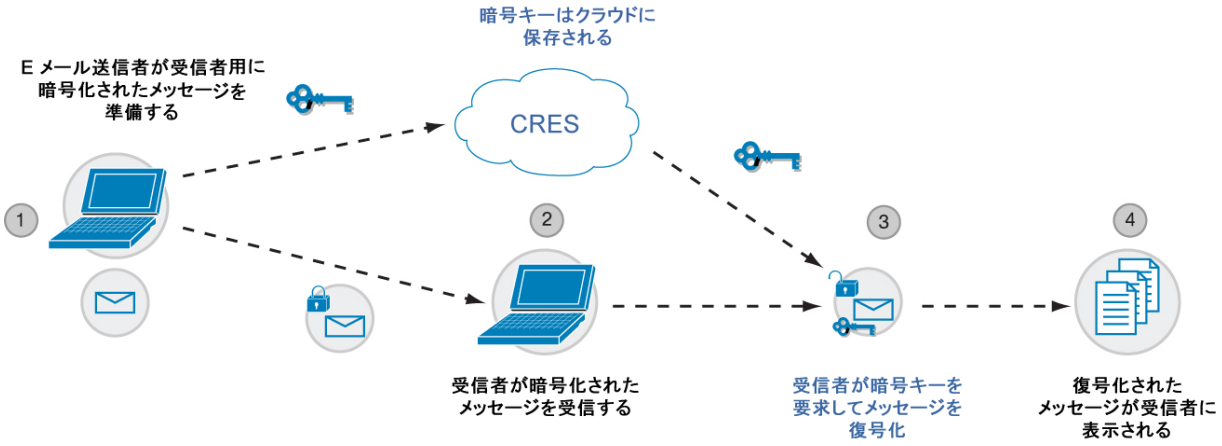
このソリューションは、ファイアウォールの外にあるインターネットでの送信中の E メールと、宛先の E メール サーバ上のストレージ内にある E メールの両方について、その中に含まれる機密性の高いビジネス情報や知的財産を保護します。

カスタマー サービスの向上

組織とその顧客は、顧客が好むチャネルを使用して、非常に優れたレベルのセキュリティで通信できます。

Registered Envelope Service を使用すれば、新しいハードウェアを導入しなくても、ターンキー方式のエンタープライズ クラス E メール暗号化ソリューションが提供されます。安全性の高い複数の配信方式によって、多様なビジネス ニーズに柔軟に対応できることに加えて、統合された管理と認証により簡単に導入できるようになっています。図 2 は、暗号化された E メール メッセージの送信と受信がユーザにとってどれほど簡単かを示しています。

図 2. ターンキー方式の E メール暗号化



導入

C シリーズ E メール セキュリティ アプライアンスで定義されたポリシーに従ってメッセージを暗号化し、復号化します。

まとめ

多くの成功事例からわかるように、Cisco Registered Envelope Service は、現代のビジネスでますます重視されるようになってきている安全性の高い通信の要件を柔軟に満たすことができる、唯一のクラウドベース暗号キー サーバです。どこからでも利用できること、柔軟な配信方法、エンタープライズ クラスの拡張性とビジネスクラスの E メールの機能により、効率的で信頼できる低価格な高セキュア通信チャネルとしてのインターネットの使用の拡大をサポートします。

関連情報

詳細については、次のマニュアルをご覧ください。

データ シート：Cisco Registered Envelope Service における複数ブランドのサポート

At-a-Glance：Cisco Registered Envelope Service

Web ページ：Cisco E メール暗号化

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-677121-04JA 16.05